Data protection in the age of welfare conditionality

Gantchev, Valery

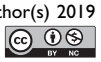
Published in:
European Journal of Social Security

DOI:
10.1177/1388262719838109

Article

EJSS

European Journal of Social Security
2019, Vol. 21(1) 3–22



DOI: 10.1177/1388262719838109
journals.sagepub.com/home/ejs


Data protection in the age of welfare conditionality: Respect for basic rights or a race to the bottom?

Valery Gantchev
University of Groningen, the Netherlands

Abstract
This article addresses the informational control powers of the state to detect social security fraud as one of the pillars supporting welfare conditionality in Western European states. It sheds light on the question of whether the repressive trend of vastly expanding conditions and sanctions attached to welfare benefits can also be observed in an unwarranted expansion of the adopted control powers of the government. The article begins by highlighting the importance of data protection law in the field of social security. It then provides a normative yardstick for assessing nationally the control powers by analysing the normative criteria set by the EU data protection framework, more specifically with regard to the purpose limitation principle and the transparency rights of individuals. Three case studies are carried out on Germany, the United Kingdom and the Netherlands which investigate the conformity of the control powers of the welfare administration with the basic right to data protection. The article concludes by providing explanations for the diverging level of protection in the examined countries and by recommending strategies for improving the data protection position of welfare beneficiaries.

Keywords
Welfare conditionality, control, privacy, protection of personal data, profiling, GDPR, SyRI

Introduction

A chief characteristic of the age of welfare conditionality is the tight link between welfare rights and claimant duties. This characteristic is, however, by no means a new phenomenon; claimant duties have always been part of social security systems in Europe. The right to social assistance

Corresponding author:
Valery Gantchev, PhD Researcher, Department of Constitutional Law, Administrative Law and Public Administration, University of Groningen, the Netherlands.
Address: PO Box 716 Groningen 9700 AS, the Netherlands.
Email: v.gantchev@rug.nl

was conceptually designed by the architects of the modern welfare state to be a conditional right which depends on the recipients' willingness, and ability, to take up paid employment.[1] The age of welfare conditionality is, however, more distinctly characterised by the profound shift that has been taking place in the balance between welfare rights and responsibilities in favour of the latter. This shift reflects a new view on the role of the welfare state which found its way into Western Europe in the last decade of last millennium. Inspired by the Scandinavian experience,[2] the social democratic parties of the 1990's embraced Giddens' 'Third Way'[3] strategy to welfare provision with the aim to 'transform the safety net of entitlements into a springboard to personal responsibility.'[4] In recent years, this process, which was initiated as creeping conditionality,[5] has reached new heights and is now being criticised by academics for its unintended effects in moral global terms as the rise of the repressive welfare state, with repressive trends subject to the spiral of formulating increasingly stricter obligations and tougher sanctions.[6] Overall, these developments challenge the post-war idea of social citizenship which is fundamental to the conception of social security as a right.[7]

From a legal perspective, welfare conditionality employs three techniques:[8] (intensified) claimant obligations, (stricter) sanctions for non-compliance and (wider) control powers of the government to monitor and investigate sanctionable behaviour. While the first two elements are enjoying growing academic attention, the research landscape pertaining to the control powers of the government has remained largely scarce. The aim of this article is to examine whether the growing repressive trend which can be observed in the areas of claimant obligations and welfare sanctions is also reflected in an unwarranted expansion of the control powers of the government.

More specifically, the article critically addresses the powers of the public administration to link and analyse the personal data of welfare beneficiaries for the prevention and detection of welfare fraud. Section 2 sheds light on the importance of automated data processing for the public administration and highlights the role of data protection in safeguarding the basic rights of citizens who are dependent on the provision of welfare benefits. Section 3 provides a normative yardstick by exploring some of the requirements which the EU data protection framework prescribes to data processing in the public sector for the purposes of welfare fraud prevention. Finally, Section 4 carries out three country-specific case studies on Germany, the United Kingdom and the Netherlands. The case studies evaluate the extent to which the adopted national control powers are in accordance with the basic right to data protection. The article concludes by elaborating on the differences between the level of protection in the examined countries and recommends strategies for improving the data protection position of welfare beneficiaries.

1. Daguerre and Etherington (2014); Watts and Fitzpatrick (2018).
2. Eichenhofer (2015: 25).
3. See Giddens (1998); for a more detailed elaboration on the philosophical underpinnings of the activating welfare state. See also Dwyer (2000) and Schwitters and Vonk (2016).
4. Blair (1998), *The Third Way: New Politics for the New Century*, as cited in: Eichenhofer (2015:24-25).
5. Dwyer (2004).
6. Vonk (2014); for an analysis on the effectiveness, impacts and ethics of welfare conditionality cf. the final findings of the Welfare Conditionality project <http://www.welfareconditionality.ac.uk/publications/final-findings-welcond-project/> accessed 10.02.2019.
7. Dwyer and Wright (2014).
8. Watts and Fitzpatrick (2018), see Chapter 3.

An important characteristic of the age of welfare conditionality is the tight link between welfare rights and claimant duties. This characteristic is, however, by no means a new phenomenon; claimant duties have always been part of social security systems in Europe. The right to social assistance was conceptually designed by the architects of the modern welfare state to be a conditional right which depends on the recipients' willingness, and ability, to take up paid employment.[9] The age of welfare conditionality is, however, more clearly characterised by the profound shift that has been taking place in the balance between welfare rights and responsibilities in favour of the latter. This shift reflects a new view on the role of the welfare state which found its way into Western Europe in the last decade of last millennium. Inspired by the Scandinavian experience,[10] the social democratic parties of the 1990's embraced Giddens' 'Third Way'[11] strategy to welfare provision with the aim of 'transforming the safety net of entitlements into a springboard to personal responsibility'.[12] In recent years, this process, which was initiated as creeping conditionality,[13] has reached new heights and is now being criticised by academics for its unintended effects in moral global terms in ushering in the rise of the repressive welfare state, with repressive trends subject to the spiral of formulating increasingly stricter obligations and tougher sanctions.[14] Overall, these developments challenge the post-war idea of social citizenship which is fundamental to the conception of social security as a right.[15]

From a legal perspective, welfare conditionality employs three techniques:[16] (intensified) claimant obligations, (stricter) sanctions for non-compliance and (wider) control powers for the government to monitor and investigate sanctionable behaviour. While the first two elements are enjoying growing academic attention, the research landscape pertaining to the control powers of the government is still largely sparse. The aim of this article is to examine whether the growing repressive trend which can be observed in the areas of claimant obligations and welfare sanctions is also reflected in an unwarranted expansion of the control powers of the government.

More specifically, the article critically addresses the administrative powers to link and analyse the personal data of welfare beneficiaries for the prevention and detection of welfare fraud. Section 2 sheds light on the importance of automated data processing for public administration and highlights the role of data protection in safeguarding the basic rights of citizens who are dependent on the provision of welfare benefits. Section 3 provides a normative yardstick by exploring some of the requirements that the EU data protection framework prescribes to data processing in the public sector for the purposes of welfare fraud prevention. Finally, Section 4 reports on three country-specific case studies on Germany, the United Kingdom and the Netherlands. The case studies evaluate the extent to which the adopted national control powers are in accordance with the basic right to data protection. The article concludes by elaborating on the differences between the levels

9. Watts and Fitzpatrick (2018); Daguerre and Etherington (2014).
10. Eichenhofer (2015:25).
11. Giddens (1998); for a more detailed elaboration on the philosophical underpinnings of the activating welfare state, cf Dwyer (2000) and Schwitters and Vonk (2016).
12. Blair (1998), *The Third Way: New Politics for the New Century*, as cited in: Eichenhofer (2015:24-25).
13. Dwyer (2004).
14. Vonk (2014); for an analysis on the effectiveness, impacts and ethics of welfare conditionality cf. the final findings of the Welfare Conditionality project <http://www.welfareconditionality.ac.uk/publications/final-findings-welcond-project/> accessed 10.02.2019.
15. Dwyer and Wright (2014).
16. Watts and Fitzpatrick (2018), see Chapter 3.

of protection in the three countries and recommends strategies for improving the data protection position of welfare beneficiaries.

2. The importance of personal data (protection) in relation to welfare fraud

The rapid digitalisation of the public sector has increased the relevance of personal data for the modern welfare state. Generally, states dispose of vast amounts of personal data spread across their administrative branches. Municipalities possess detailed personal records relating to the living situation of beneficiaries, tax authorities can reveal information about any (side-) income of individuals, and unemployment agencies have data on previous periods of unemployment. By processing the relevant personal data, the welfare administration can easily determine whether a recipient of social assistance has fulfilled the conditions attached to the benefit, or whether he or she has provided the administration with incorrect information. In practice, the welfare administration collects the necessary personal information from the relevant public bodies and links it together in order to analyse it with the help of algorithms. The automation of this process significantly increases the efficiency of the operation, which can be completed within a fraction of the time that would be needed to carry out a comparable analysis manually.

While it must be acknowledged that the use of automated data processing techniques increases the efficiency of welfare administration when investigating benefit fraud, it must be also pointed out that such practices may have adverse effects on the legal position of citizens. These effects are very well illustrated in the *Census*-judgment[17] of the German Federal Constitutional Court from 1983, which laid the foundation for the country's national data protection framework. As duly noted by the Court, the shift from manual processing of personal information stored on paper towards automated processing has enabled the state to process much larger amounts of personal data nearly instantaneously and regardless of the distance between the locations where the data are stored. Furthermore, the potential to link personal data allows governments to create very detailed personal profiles without allowing citizens to exercise control over their accuracy or the use of their personal data. The Federal Constitutional Court observed that this 'previously unseen' expansion in the possibilities for the state to process personal data exerts 'psychological pressure' on individuals which may prompt them to adapt their behaviour. This touches on the right of citizens to develop and protect their personality within an autonomous area of private life. From the point of view of personal autonomy and (informational) self-determination, citizens should be able to foresee and control the potential uses of their personal data.

The considerations of the German Federal Constitutional Court sketched above prove to be especially relevant in the sensitive area of social security. A primary function of social security is to prevent social exclusion that, according to its definition, 'precludes full participation in the normatively prescribed activities of a given society and denies access to information, resources, sociability, recognition, and identity, eroding self-respect and reducing capabilities to achieve personal goals.'[18] The abolition of discriminatory and degrading treatment of people who are dependent on the payment of welfare benefits is an important factor in the promotion of social inclusion. Extensive control measures signal a lack of trust in the state by its most vulnerable

17. German Federal Constitutional Court 15.12.1983, BVerfGE 65, 1.
18. Silver (2007:1).

citizens, which underpins the urge to increasingly monitor their behaviour. This approach can be counter-productive for the social reintegration of beneficiaries because it reinforces the existing stigmatisation of benefit claimants by openly questioning their trustworthiness.

In summary, the automated processing of personal data is an important, efficient tool which the modern welfare state has at its disposal in the legitimate effort to counteract the irregular use of welfare benefits. At the same time, however, the inflation of governmental informational powers can have a significant negative impact on the private lives of beneficiaries and on the inclusive function of social security. One of the main objectives of data protection reveals itself here – to strike a balance between the public interest pursued by the processing of personal data and the basic rights of the individual concerned. The next section examines the mechanisms employed by the EU data protection framework to this end.

3. The EU framework on data protection

3.1 The EU General Data Protection Regulation (GDPR)

The GDPR[19] lies at the heart of the EU data protection framework. It came into force in May 2018, the Regulation with the objective of ensuring a consistent and high level of protection for individuals with regard to their personal data. Accordingly, it has a wide scope of application,[20] which covers both the private and the public sector. Personal data is defined very broadly as 'any information relating to an identified or identifiable natural person.' The term 'processing' can also be broadly interpreted – it covers any set of operations that is performed on personal data, including their collection, organisation, storage, adaptation, retrieval, erasure or destruction. The Regulation refers to the person whose data are being processed as the 'data subject' while reserving the term 'data controller' for the body responsible for the processing of personal data. The data controller determines the purposes and the means for processing and can be a natural or legal person, as well as a public authority or an agency.

The GDPR allows personal data to be processed only when this is in accordance with the core principles of data protection laid down in Article 5, the first three of which are briefly described for the purposes of this article. The principle of lawful, transparent and fair processing requires that the collection and further processing of personal data are based on a legal ground and that the data subjects are informed about the use to which their data is put. Furthermore, the purpose limitation principle requires that personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes. The related principle of 'data minimisation' prescribes that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The core principles of data protection in Article 5 GDPR are formulated in a very general manner, however, and the remaining provisions of the Regulation provide a certain degree of concretisation that is required for their application in practice.

Article 6 GDPR defines the qualitative requirements which apply to the legal grounds for the processing of personal data. With specific attention to the public sector, the Regulation allows

19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
20. Cf. Articles 1-4 GDPR.

national bodies to process personal data without the consent of the data subject when this is based on national legislation.[21] The respective legal acts are subjected to a proportionality test in order to ensure that the state administration does not collect and process more personal data than is strictly necessary for achieving the purpose of the data processing.[22] The purpose for which personal data is processed thus provides an important point of reference when applying the abstract proportionality test to the legal ground on which the operation is based. It gives an indication of the necessary extent of the data processing, including the categories of personal data that need to be processed. By doing so, it makes possible the application of the proportionality test and the examination of the lawfulness, fairness and transparency of the data processing operation.

The focus of this section is directed at examining two sets of requirements which are particularly important in the context of the control powers used by governments for welfare fraud prevention. In the first place, the purpose limitation principle and its implications are examined. As noted above, this principle is of central importance to the application of other data protection safeguards and, therefore, is a key factor to the effective protection of personal data in general. In the second place, this section examines the transparency rights of welfare beneficiaries which are an indispensable tool for ensuring that citizens remain in control of their data.[23] Finally, it critically addresses the notable exceptions made by the GDPR to the application of the purpose limitation principle and the transparency rights of individuals in the field of social security.

3.2 The purpose limitation principle

In the words of Article 5(1)(b) GDPR, the 'purpose limitation principle' requires that personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with these purposes.[24] Due to a lack of relevant case law and policy documents, the most feasible way to gather further information on the required degree of purpose is to consult the opinion on purpose limitation of the EU data protection advisory body Article 29 Working Party (WP29).[25]

The 'purpose limitation principle' builds on the notion that the purposes of the data processing must be *explicit* and *specified*. The 'criterion of explicitness' demands that the purposes for the processing of personal data be clearly revealed, explained or expressed in some intelligible form.[26] The specification criterion requires that the purposes be sufficiently defined to enable the implementation of any necessary data protection safeguards and to delimit the scope of the processing operation. The controller must carefully consider what purposes the personal data will be used for and must not collect personal data that are not necessary, adequate or relevant for the purposes that are intended to be served.[27]

21. Articles 6(1)(c) and (e) GDPR.
22. The proportionality test in embedded in Articles 6(1)(c) and (e) GDPR.
23. Klingenberg (2016:107); Westin (1970).
24. The latter requirement of compatibility is weakened in cases where personal data is processed in the public interest based on national legislation, cf. Recital 50 GDPR.
25. Established in 1996, WP29 was replaced by the European Data Protection Board (EDPB) with the entry-into-force of the GDPR in May 2018.
26. WP29 (2013:17).
27. WP29 (2013:15).

In the words of the WP29 advisory body, a purpose that is vague or general will usually not meet the criteria of being specific.[28] Obviously, the required degree of specification calls for a case-by-case examination in which all relevant circumstances are considered. The WP29 has provided practical examples of purpose formulations that it considers too general: 'marketing purposes', 'IT-purposes' and 'future research'.[29] All these purposes share the feature that they can easily be specified further by providing more detail: Which kind of marketing, which area of IT and which type of research? These examples show that a purpose formulation will not satisfy the requirement of purpose specification if its scope can easily be narrowed down by providing further details regarding the particular field or the context in which it applies.

The general guidelines provided by the WP29 advisory body can be transposed to the situation of welfare fraud investigation to extract the criteria that can be applied to the underlying national legislation. Firstly, the national legislation in question must satisfy the requirement of explicitness by establishing a link between the processing of personal data and the purposes that it serves. When consulting the respective legislation, citizens must be able to recognise that their personal data is collected and examined for the purposes of fraud investigation.

Secondly, the purpose of the national legislation must meet the requirements of specification. In the light of the examples discussed above, a general, broad purpose formulations such as 'fraud investigation in social security' should be considered too vague to satisfy the specification criterion. This purpose formulation can be further specified by determining the field of social security in which fraud is being investigated. Social security is a bundle of arrangements put into place to provide relief against occurring social risks. The array of covered social risks is a wide one, ranging from (temporary) unemployment and sickness to child support, old-age and social care. Each of these arrangements has its own distinctive characteristics, and this is reflected in the conditions attached to the benefits, which vary across different social security schemes. It is important to acknowledge this divergence in the benefit conditions because it leads to the conclusion that the government needs to collect and analyse *different* sets and categories of personal data in order to detect non-compliance under the various social security schemes: The welfare administration might have legitimate reasons to know the water and electricity consumption of a benefits recipient under a needs-based scheme (social assistance), however this information would be completely irrelevant under an unemployment insurance scheme.

These practical examples bring us back to the essential function of the purpose limitation principle, which the WP29 once labelled as the 'cornerstone of data protection.'[30] Some of the central safeguards in data protection law can only be applied effectively when the purposes of the data processing are specified with sufficient precision. When applying the proportionality test to a broadly formulated purpose such as 'fraud investigation in social security', the range of personal data that may be considered necessary to collect and further process is much greater compared to narrower, sector-specific purpose definitions such as 'fraud prevention in unemployment insurance'. By adopting legislation that pursues such general purposes, governments maximise the outreach of their control powers while simultaneously undermining the data protection rights of the concerned individuals. From the perspective of an effective application of the purpose limitation principle and other data protection safeguards, governments should be held responsible for

28. WP29 (2013:16).
29. P29 (2013:16).
30. WP29 (2013:4).

adopting legislation which pursues well-defined, explicit and narrow purposes for the processing of personal data. National legislation that supports the control powers of the government should be limited to specific social security arrangements. This would set reasonable limits on the scope of the control powers of the government. Furthermore, as we shall see in the next section, this would also benefit the transparency rights of welfare recipients.

3.3 Transparency rights of welfare recipients

As already mentioned, the function of the purpose limitation principle is not only to set limits on the scope of the processing operation, but also to facilitate the meaningful exercise of some of the other data-subject rights enshrined in the GDPR. An important cluster of rights relates to the transparency of data processing that is one of the central principles of the GDPR laid down in Article 5(1). The concrete requirements for safeguarding the transparency of data processing can be found in Section 2 of the GDPR ('Information and access to personal data'). Articles 13 and 14 GDPR specify the information duties for data controllers when processing personal data. The main difference between the two provisions lies in their scope of application. Article 13 applies to the situation where the personal data are collected from the data subject, while Article 14 covers the cases where the processed data have not been obtained from the data subject. Article 15 GDPR, in turn, establishes the corresponding right of access which guarantees the access of data subjects to the relevant information relating to the processing of their personal data. As Wachter *et al* put it, '[t]ogether, Articles 13-15 form what has been called the 'Magna Carta' of data subject's rights to obtain information about the data help about them, and to scrutinize the legitimacy of the data processing.'[31]

The array of information covered by the transparency rights of data subjects under the GDPR is a broad one. Welfare beneficiaries have the right to know the identity of the controller of their personal data and the purposes of the data processing as well as the categories of personal data concerned.[32] Furthermore, the welfare administration must provide additional information in cases where it is making use of automated decision-making (including profiling[33]) within the meaning of Article 22 GDPR: Data subjects have the right to be made aware of the use of these techniques and furthermore receive meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.[34] Research carried out by Wachter *et al* conclude that the practical added value of this right is limited and that it does not amount to what is dubbed in academic circles a 'right to explanation of automated decision-making.'[35] The first limitation lies in Article 22 GDPR which requires that a decision is based *solely* on automated processing. In cases where (nominal) human intervention has taken place, the respective transparency right of the data subject does not apply. Nevertheless, even if a particular case does fall under the scope of application of Article 22 GDPR, the 'meaningful information' is limited to an *ex ante*

31. Wachter, Mittelstadt and Floridi (2017:83); also cf. the academic literature referred to in fn. 33 above.
32. Cf. Articles 13(1), 14(1) and 15(1) GDPR.
33. Profiling is defined in Article 4(4) GDPR as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects [. . .]'
34. Cf. Articles 13(2)(f), 14(2)(g) and 15(1)(h) GDPR.
35. Wachter, Mittelstadt and Floridi (2017).

explanation of system functionality instead of an *ex post* explanation of the exact logic used by an algorithm to reach a specific decision.[36]

3.4 Data protection in the limbo of 'margin for manoeuvre'

An unavoidable characteristic of law is that not all requirements that are desirable from a theoretical point of view are always translated into practice. The EU law-making process is subject to national influences, which may result in the introduction of exceptions for certain situations. The adoption of the GDPR is a good example of such political compromise – the original proposal submitted by the Commission[37] was subject to a record number of amendments (over 3000) before it could pass in the parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE).[38] More amendments were agreed on later in the lifecycle of the decision-making process by the European Council and European Paraliament.[39]

Some of the amendments were clearly pushed forward with the objective of limiting the scope of the safeguards initially proposed by the Commission with regard to cases where governments process personal data in the public interest. The legal instrument to facilitate this was found in the old formula 'margin for manoeuvre'. This formula is a remnant of Recital 9 of the EU Data Protection Directive:[40] 'Member States will be left a margin for manoeuvre [. . .] whereas, within the limits of this margin for manoeuvre [. . .], disparities could arise in the implementation of the Directive.' The practical implications of this 'margin for manoeuvre' under the Directive were initially left unclear. In 2003, the Court of Justice of the EU (CJEU) adopted its *Lindqvist* judgment in which the Court addressed the balance between the full harmonisation of data protection in the EU and the 'margin for manoeuvre' for Member States in abstract terms:[41]

> It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life.

Initially, the margin for manoeuvre was not included in the Commission's proposal, which revolved around the concept of full harmonisation. However, the subsequent amendments made by the European Parliament and the European Council resulted in important reservations being made to the full degree of harmonisation. Recital 10, which formulates the objective to 'ensure a consistent and high level of protection' that 'should be equivalent in all Member States,' was altered to include the formula of margin for manoeuvre. The new wording of Recital 10 allows Member States to 'maintain or introduce national provisions to further specify the application of

36. Wachter, Mittelstadt and Floridi (2017).
37. Proposal for a Regulation of the European Paraliament and of the Council 25.10.2012, COM(2012) 11.
38. A comprehensive list of all amendments and a break-down per country or MEP can be found on <https://lobbyplag.eu/map/articles> accessed 10.02.2019.
39. Cf. for a comparaison of the texts adopted by the European Parliament and the European Council: <https://edri.org/files/EP_Council_Comparaison.pdf> accessed 10.02.2019.
40. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
41. CJEU 06.11.2003, C-101/01 (Lindqvist), para 97.

the rules of t[he] Regulation' when processing personal data in the public interest. This line of thought is further consolidated in Article 6 GDPR which governs the applicable legal grounds for the processing of personal data. On the initiative of several German Members of the European Parliament,[42] paragraph 3 was amended to allow national governments to pass national legislation which 'adapt[s] the application of rules' of the GDPR. The list of rules which can be adapted is long and touches on nearly every aspect of the EU data protection framework:

> [. . .] *inter alia*: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX [. . .]

In the context of the present article, the ability to limit the applicability of the purpose limitation principle is especially worrisome. This restriction can be used by national governments to pass broad 'container' legislation that allows them to process more personal data than strictly necessary.[43] This affects not only the scope of the control powers of the government, but also has a negative impact on the application of the proportionality principle and the exercise of the transparency rights of data subjects. With regard to the latter point, Article 23 GDPR creates another notable limitation: when acting in the public interest, national governments are allowed to restrict the transparency rights of the data subject. Article 21(1) GDPR provides a list of areas in which such restricting measures can be adopted. The amendments passed by the European Council made this list more explicit – 'taxation matters' was changed to 'other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters, public health and *social security* [. . .]' (emphasis added by author).

Until the present day there is a lack of clarity on the motives of the EU legislator for resurrecting the margin for manoeuvre formula with all its restricting implications. Taking into consideration that the important amendments to Article 6(3) GDPR were made by German MEPs, one assumption is that the leeway for member states was created in response to concerns that the introduction of the GDPR could have a negative impact on the high level of data protection that was already established in some countries prior to the Regulation.[44] By allowing national legislation to further specify the rules of the GDPR, these countries could continue pursuing the high standards of national protection. This, however, is a double-edged sword. By effectively limiting the extent of full harmonisation, the margin of manoeuvre and related limitations that allow certain member states to offer a higher standard of protection, but are simultaneously counterproductive for other countries which, for one reason or another, fail to deliver the desired level of protection.

4. Country-specific case studies

To shed light on the application of data protection standards in the contemporary welfare state, this Section presents three case studies that were carried out on Germany, the United Kingdom and the

42. Cf. Amendment LIBE #931 <https://lobbyplag.eu/map/discuss/libe/931> accessed 10.02.2019.
43. Cf. also Recital 45 GDPR.
44. Such concerns were expressed in Germany by Britz (2009), Burgkardt (2013:420), Massing (2012).

Netherlands. These countries were chosen because of their close geographical proximity and their strongly divergent legal traditions. The case studies examine the mechanisms that have been used by national governments to link and analyse personal data in the fight against welfare fraud. In addition to describing the functioning of these mechanisms, the analysis examines whether the underpinning national legislation and its implementation in practice by the welfare administration is in accordance with EU data protection standards, more specifically with regard to the purpose limitation principle and the transparency rights of welfare beneficiaries.

4.1 Germany

Over the years, Germany has gained the reputation as one of the frontrunners in data protection. In 1970, the state of Hesse enacted the world's first data protection law[45] which paved the way for the German Federal Data Protection Act (BDSG)[46] almost 8 years later. In 1983, the German Federal Constitutional Court adopted its landmark decision in the *Census-case*[47] in which it recognised the right to informational self-determination as a basic right with a legal anchor in the national constitution (Articles 2(1) and 1 German Basic Law).[48] Furthermore, the German framework pays special attention to data protection in the field of social security. This is partially due to the principle of confidentiality of social security data,[49] which builds on the notion that welfare recipients should not suffer a degradation in the standard of data protection when compared to other citizens solely by reason that their livelihood depends on welfare benefits.[50] For that purpose, the German legislator has introduced a separate data protection regime which applies specifically to welfare arrangements. The relevant rules are codified in national social security legislation acts and a common framework is established in §§ 67-85 Sozialgesetzbuch X (SGB X). These specific rules take precedence over the general data protection regime, which is regulated in the German data protection act (the Bundesdatenschutzgesetz).

German social security legislation contains two legal grounds that allow the welfare administration to periodically link and examine large sets of personal data in the battle against the illegitimate use of welfare benefits: § 52 SGB II and § 118 SGB XII. § 52 SGB II applies to the general unemployment assistance scheme known as Hartz IV. Based on this provision, the competent public bodies are obliged to transfer, link and examine personal data four times every year. Strictly speaking, the purpose of the data processing is not defined explicitly in the legislative provision, which is a noticeable shortcoming.[51] Nevertheless, the purpose definition can be established contextually, by means of systematic interpretation.[52] Furthermore, the principle of data minimisation seems not to have been impacted negatively by the lack of explicit purpose definition. The scope of personal data that can be processed under § 52 SGB II is limited to what is strictly necessary to control compliance under the general social assistance scheme. It covers

45. Hessisches Datenschutzgesetz 07.10.1970, GVBl. II 300-28.
46. Bundesdatenschutzgesetz 01.01.1978, BGBl. I 1977, 201.
47. German Federal Constitutional Court 15.12.1983, BVerfGE 65, 1.
48. For a detailed examination of (the evolution of) the various constitutional data protection safeguards in Germany cf. Burgkardt (2013:85-244).
49. The principle of confidentiality of social security data is laid down in § 35 SGB I.
50. Fromm (2013), § 52 SGB II, nr 9.
51. Schmidt (2018), § 52 SGB II, nr 9.
52. The necessary context is provided by Chapter 6 SGB II and § 50 SGB II.

information on other welfare benefits that an individual receives, general taxation data and a minimum of personal identification data – name, place and date of birth, address and social insurance number.

§ 118 SGB XII creates a similar competence for compliance control under the social assistance schemes that are regulated in SGB XII. These schemes form the outermost safety net of the German welfare system and can be relied on by people whose basic needs are not covered by other welfare arrangements. There are several important differences between the legal ground in question and § 52 SGB II. In the first place, the decision to analyse personal data is subject to the discretion of the responsible bodies that can, but are not obliged to, carry out the data operations 'frequently'. Secondly, § 118(4) SGB XII contains an explicit formulation of the purpose of the data processing: The prevention of the illegitimate use of benefits under one of the social security arrangements regulated in SGB XII. Also, the scope of personal data that can be processed is modified in accordance with this purpose definition. Furthermore as regards information about benefits paid under other social security schemes and general taxation data, § 118 SGB XII allows the processing of information regarding the costs for rent, electricity, gas, water and garbage disposal.

The examination above demonstrates that § 52 SGB II and § 118 SGB XII are designed in a sector-specific manner, in accordance with the purpose limitation principle of EU data protection law. As a result, the scope of personal data that can be processed by the responsible public bodies is limited to what is strictly necessary for controlling compliance under the particular social security system. This effectively sets limits on the scope of the control powers of the welfare administration and benefits the transparency rights of welfare beneficiaries. Nonetheless, there used to be a debate in German academic circles about whether the data matching powers in the SGB are in accordance with the basic right to informational self-determination guaranteed by the Social National Constitution.[53] In 2015, the German Federal Court confirmed the constitutionality of § 52 SGB II.[54] As one of the decisive factors influencing this decision, the court pointed at the restrictive, sector-specific design of the provision which aligns with the principle of specificity.[55]

4.2 The United Kingdom

The analysis of personal data for the prevention and detection of welfare fraud has become common practice in the UK since it was introduced for the first time in the mid-1990s. Every two years, the British government carries out a massive data matching exercise under the National Fraud Initiative (NFI). The bi-annual exercises make use of data supplied by over 600 public authorities, including health authorities and government departments, as well as a growing number of private-sector bodies.[56] The initial focus of the NFI was on fraud in housing benefit and student award claims. However, the scope of the initiative has become much wider and now covers various public programmes, ranging from pensions and personal budgets to licenses for taxi drivers and

53. The constitutionality of these powers is accepted by Merten (2018), § 52 SGB II, nr 2; Hirschboeck (2004: 594-595); and rejected by Kunkel (1995).
54. German Federal Social Court 24.04.2015, B 4 AS 39/14 R.
55. In German constitutional law this principle is known as *Bestimmtheitsgebot.*
56. Bellamy *et al* (2005: 401).

market traders, public sector payroll and transport permits.[57] The current 2018-2019 exercise does not address unemployment benefit fraud, but nevertheless the British government has indicated its intention to do so by including Universal Credit in the scope of the data matching exercises.[58]

The legal framework underpinning the NFI is embodied in Schedule 9 of the Local Audit and Accountability Act 2014. It empowers the Cabinet Office to conduct data matching exercises which, according to the statutory definition, involve a comparison of sets of data to determine how far they match (including the identification of any patterns and trends).[59] The scope of personal data which can be collected under this Act is practically unlimited. The Cabinet Office can collect personal data which may 'reasonably' be required for the purpose of conducting data matching exercises from any relevant national authority.[60] The provision of the data by the authority is mandatory. Nevertheless, if the Cabinet Office considers it appropriate, it can also collect personal data from any other 'body or person,' both in and outside of England.[61] The provision of personal data in this case is voluntary.

The practically unlimited powers which national legislation confers on the public administration are specified in a variety of non-binding governance arrangements that have been adopted by the Cabinet Office.[62] The most important one is the Code of Data Matching Practice which lays down a framework that can be applied to the whole lifecycle of a data matching exercise.[63] With regard to the criteria for selecting the relevant personal data for a particular exercise, the Code states that the Cabinet Office will only choose data sets that are to be matched where it has reasonable evidence to suggest that fraud may be occurring and this fraud is likely to be detected as a result of matching those data sets.[64] Furthermore, the scope of the data which can be processed must be limited to the minimum needed to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality to meet the purpose of preventing and detecting fraud.[65] Some additional information, for example on the rights of the data subject, is included in the recently revised privacy notice of the NFI.[66]

The Cabinet Office regularly adopts and publishes data specification for every matching exercise.[67] The latest version applies to the 2018-2019 exercise. The scope of personal data that can be processed is clear and well delimited, as the data specification applicable to personal budgets demonstrates.[68] Besides some basic personal information needed to determine the identity of

57. For an overview of the scope of the 2018-2019 exercise cf. <https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-specifications>.
58. Cabinet Office (2016: 23).
59. Schedule 9 paraa. 1 Local Audit and Accountability Act 2014.
60. Schedule 9 paraa. 2 Local Audit and Accountability Act 2014
61. Schedule 9 paraa. 3 Local Audit and Accountability Act 2014
62. The various reports and guidance documents are published online at <https://www.gov.uk/government/collections/national-fraud-initiative>.
63. Cabinet Office (2018).
64. Cabinet Office (2018), para 2.5.1.
65. Cabinet Office (2018), para 2.6.1.
66. See https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text.
67. For a clear overview of the data specifications applicable to the 2018-2019 exercises in the public sector cf. https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-specifications.
68. See <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/6963%2095/Personal_Budgets_Data_Spec_18_19.pdf>.

persons and their place of residence, it includes identifiers such as the person's national insurance number, the unique property reference number and the claim reference number, as well as information regarding payments that were made in the past and payments made under other social security programmes (such as housing benefit and pensions income).

Overall, the non-binding governance instruments adopted by the Cabinet Office compensate for the notable shortcomings displayed by the extremely broad primary legislation. The purposes of the data processing are defined in a restrictive manner, and the categories of processed data are sufficiently specified. As a result, the scope of the data processing operations under the NFI is limited to the minimum necessary for revealing fraud under a specific public benefit scheme. From this perspective, the established practice resonates with the normative requirements posed by the purpose limitation principle of EU data protection law. Furthermore, the publicity given by the British governments respects the transparency rights of welfare recipients.

4.3 The Netherlands

The track record of the Dutch government in data protection issues surrounding welfare fraud is far from flawless. In 2003, a cooperation unit[69] was established in the Netherlands between various welfare administrative bodies, the tax authority, the Ministry of Justice, the police, the public prosecutor's office and a number of municipalities. The purpose of this unit was to combat illegal work, welfare fraud, and tax fraud by leveraging the potential of linked personal data to create risk profiles. This immediately came to the attention of the Dutch Data Protection Authority (DPA), which adopted a document highlighting the various data protection rules in the context of welfare fraud prevention, with a specific focus on the scope of data processing as defined by the proportionality principle and the transparency rights of individuals.[70]

In 2007, the Dutch DPA examined one of the early schemes deployed by the cooperation unit – project *Waterproof*. Within this project, the government linked the personal data of 35,000 citizens to investigate their water consumption as an indicator of possible address fraud, which eventually resulted in the detection of 42 fraud cases (a percentage of 0.12 per cent).[71] The findings of the DPA raise a number of concerns: In all of the cases, the investigation was carried out without prior suspicion of fraud, the purpose limitation principle was not respected due to the lack of appropriate legislation, and the transparency rights of individuals were breached.[72] The Dutch government made an attempt to partially remedy these concerns by introducing the so-called *Black Box*-method, which meant that personal data would first be anonymised before being linked and examined. Additionally, the new approach failed to address the issue of the non-existent legal basis and the neglected transparency rights of the data subjects, which triggered another very critical decision of the Dutch DPA in 2011.[73]

The interventions by the DPA prompted the Dutch government to revise its data matching projects and provide them with a legal basis. This led to the birth of the project-based *System for Risk Indication* (*Systeem Risico Indicatie* / SyRI).[74] Each SyRI-project contains a predefined risk

69. Known, in Dutch, as *Landelijke Stuurgroep Interventieteams*, this cooperation is now codified in Article 64 Wet SUWI.
70. CBP (2006).
71. Inspectie SZW (2012), 12-22.
72. CBP (2007).
73. CBP (2011).
74. Article 65 Wet SUWI and Chapter 5a Besluit SUWI.

model which is based on indicators suggesting a higher probability that a person is committing benefit fraud. The collected personal data are encrypted and then linked together by the body that is responsible for carrying out the analysis. If the analysis indicates a match with the predefined risk model, the respective personal data are decrypted and transferred back to the welfare administration, which adds the risk notifications to a central register where these are kept for a period of two years. During this period, the notifications are accessible to the responsible administrative bodies which can carry out further investigation on a case-by-case basis.

As far as purpose limitation and data minimisation are concerned, SyRI displays noticeable shortcomings. The specification of the purposes served by the system can be found in Article 64(1) Wet SUWI: 'For the purpose of an integral governmental approach in the fight against the illegitimate use of public funds and public provision in the area of social security, tax supplements, the fight against tax fraud and premiums fraud and the compliance with labour legislation [. . .]' This purpose formulation is very extensive and is not confined to a specific social security scheme. As a matter of fact, data processing under SyRI is not even limited to the whole body of social security arrangements, but also addresses issues of general taxation and labour law (e.g. compliance with minimum wage regulation). The Ministry of Social Affairs and Employment displayed an awareness of the wide scope of SyRI and tried to justify it in the following statement: 'The choice for a broad purpose limitation is a conscious one and it aims to facilitate an integral approach by the government against illegitimate use, fraud and non-compliance with national legislation.'[75] Nevertheless, a 'broad purpose limitation' is a *contradictio in terminis* which is clearly incompatible with the basic principles of data protection.

The 'broad purpose limitation' is reflected in the wide scope of personal data which is collected, linked and examined with the help of SyRI. Article 5a.1(3) Besluit SUWI defines 17 broadly formulated categories of personal data: employment data, data on administrative sanctions, fiscal data, data on real estate property, data on grounds of exclusion from welfare benefits, trade data, address data, identification data, data related to the integration of foreigners, historical data concerning compliance, educational data, pensions data, reintegration data, debt data, data concerning the enjoyment of social security benefits, data concerning permits and health insurance data. The broad scope of personal data which can be processed in SyRI is among the main points criticised by the DPA and the Dutch Council of State.[76] The latter body observed:[77]

> These categories are broad and extensive, and the data which falls thereunder can, in some cases, seriously interfere with the private sphere of an individual. The definition of the categories of personal data is meant to set limits on data processing (principle of data minimisation) but, in this case, the scope is so broad that it is hard to think of a category of personal data that does not fall under it. It looks as if this definition of processed personal data does not aim to set limits, but rather to confer the broadest powers possible.

These concerns of the Council of State were disregarded by the Ministry of Social Affairs and Employment in a pragmatic fashion.[78] The Ministry explained that national legislation requires each application for a new SyRI-project to specify the purpose of the particular project, based on a

75. Kammerstukken Tweede Kamer der Staten-Generaal 2012-2013, 33 579, nr: 36.
76. CBP (2014); Raad van State (2014).
77. Raad van State (2014), point 2(a); translated by the author.
78. Ministerie van Sociale Zaken en Werkgelegenheid (2014).

determination of the scope of the necessary personal data. In the words of the Ministry, 'because the selection of relevant personal data differs in each project, it is not possible to specify it in legislation for all individual projects.'[79]

While it is true that Article 5a.1(2) Besluit SUWI prescribes the specification of the purposes of each SyRI-project along with the relevant personal data, in practice this process takes place behind closed doors. Since the launch of SyRI in October 2013, the Dutch government has initiated only three projects, one of which was cancelled prematurely. The first information about these projects reached the public after a group of lawyers filed in several freedom of information requests.[80] The government awarded the requests only partially released limited information. What becomes clear from project applications is that the investigation is directed specifically at several socially weak neighbourhoods in Eindhoven and in the Rotterdam area. A look in the application document for the project in Eindhoven clearly shows that the information provided does not specify the concrete purposes of the project and the exact categories of personal data which are being processed.[81] Instead, it vaguely describes social problems in one of the neighbourhoods of the city such as 'fraud and non-compliance with labour legislation' that need to be tackled in order to 'improve liveability in the neighbourhood.' With regard to the specification of the processed personal data, the project application refers to a so-called 'risk model for neighbourhood action'[82] that contains a definition of risk indicators used by the SyRI-projects, providing some insight into the logic and algorithms involved. The corresponding document, however, was not made publicly accessible by the Dutch government.

Today, SyRI has evolved into a highly controversial issue. In March 2018, a group of human rights organisations and several prominent individuals filed a court case against the use of SyRI by the government.[83] The list of legal grounds on which the system has been challenged is long. The most important grounds relate to the scope of the powers, the broad purpose formulation, the unclear categories of personal data and the secret algorithms for compiling the risk profiles. In May 2018, Members of the Dutch Parliament confronted the Minister of Social Affairs with critical questions regarding the use of secret algorithms.[84] The expressed concern that the logic underpinning risk profiles should be made publicly available in order to prevent biases and potential discrimination was countered by the Minister with the argument that this would give criminals an advantage. In June 2018, a subsequent motion to at least allow technical audits of the used algorithms was blocked by the Secretary of State on similar grounds. The negative attitude of the Dutch government towards preserving the well-kept secrets surrounding SyRI carried on in January 2019, when the Secretary of State refused to answer parliamentary questions concerning both the internal workings of the system, as well as its concrete outcomes in the various projects.[85] The

79. Ministerie van Sociale Zaken en Werkgelegenheid (2014: 3); translated by author.
80. The documents which were made accessible in response to the information requests can be found online on <https://www.rijksoverheid.nl/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri>.
81. The application for the SyRI-project can be found online on <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/wob-verzoeken/2017/06/14/besluit-wob-verzoeken-over-syri/1+-+21+%28Bestanden+GALOP%29.pdf>.
82. Risicomodel wijkgerichte aanpak.
83. Cf. <https://deikwijs.nl/wp-content/uploads/2018/03/dagvaarding-bodemprocedure-syri-27-maart-2018.pdf>.
84. Cf. <https://bijvoorbaatverdacht.nl/kabinet-geen-openbaring-syri-algoritmen/>.
85. Cf. <https://bijvoorbaatverdacht.nl/kamervraag-beantwoording-syri-in-capelle/>.

complete rejection of any form of accountability of the Dutch government towards the legislator regarding the bulk profiling of welfare beneficiaries is worrisome and unexplainable.

5. Conclusions

In the contemporary age of welfare conditionality, systems that link and analyse personal data are an indispensable tool in the fight against welfare fraud in Western Europe. This article reports on three country-specific analyses in order to examine whether the general repressive trend reflected in the adoption of more detailed claimant obligations and ever stricter sanctions is also accompanied by an unwarranted expansion of the respective control powers. The examination shows that, in each of countries examined here, national legislation has been adopted which provides the legal basis for the powers of the government to control compliance with conditions attached to welfare benefits. Nevertheless, the particular outcomes of the case studies are fundamentally different, and this can partially be explained in terms of the divergent legal traditions in Germany, the United Kingdom and the Netherlands.

In Germany, the strong constitutional embedding of the right to informational self-determination and the acknowledgment that welfare beneficiaries represent a vulnerable group that requires elaborate data protection rights, have translated into privacy-friendly legislation. By adopting sector-specific legislation, which clearly specifies the processed personal data and limits it to an absolute necessary minimum, the German legislator has set clear boundaries to the control powers of the state and has furthermore ensured that the anti-fraud systems operate in a transparent manner.

In the United Kingdom and the Netherlands, the legislators have chosen a more pragmatic approach by enacting broad legislation that creates practically unlimited powers for the welfare administration and simultaneously delegates the task to scope these powers to the executive. In the United Kingdom, the administrative acts that have been adopted live up to these expectations and the system, as a whole, respects the most important principles of the GDPR. The various NFI data matching exercises are accompanied by extensive policy documents. The non-binding guidelines clearly specify which personal data is processed per exercise, and the information made public by the British government ensures that transparency rights are respected.

In the Netherlands, the implementation of SyRI into practice displays alarming shortcomings. SyRI is the most privacy-intrusive anti-fraud system in the three countries examined in this article since it employs risk profiles to flag individual citizens. The negative impact of this on the right to data protection is amplified by the extremely broad scope of data processing possible under SyRI. When adopting the underlying legislation, which requires that the control powers are more clearly defined in the applications for the particular SyRI projects, the Dutch legislator was clearly aiming for more flexibility. In reality, this mechanism proves to be a dangerous failure. The existing project applications do not formulate specific purposes for the processing and the categories of processed personal data remain unclear. What might at first sight appear as a display of sloppiness turns out to be something much more worrying? After a number of parliamentary inquiries and freedom of information requests, the Dutch government still continues to deliberately prevent the release of information to the public concerning the processed categories of personal data, the logic of the algorithms and the outcomes of the projects.

While it is true that the GDPR provides the necessary leeway for Member States to neglect some core aspects of its rules when processing personal data for welfare fraud prevention, this approach is highly undesirable from the perspective of the right to social security. Any deviation from the

standards of protection effectively means that welfare beneficiaries are subject to a lower level of basic rights protection as compared to 'regular' citizens who are not dependent on state support. This is problematic in light of the effective exercise of the internationally protected right of social security and social assistance[86] which requires that welfare beneficiaries 'should not be prevented from exercising their civil and political rights in full.'[87]

Considering that the adoption of the GDPR was a politically cumbersome process and that social assistance is traditionally a sensitive matter, the expectation that the CJEU would directly scrutinise national legislation to restore the balance is unrealistic. Nevertheless, the Court could intervene in more indirect ways. One solution, which would help strengthen the position of welfare beneficiaries, would be to require Member States to enact legislation that explicitly specifies (the scope of) the limitations imposed on the basic right to data protection. This would ensure that such limitations are transparent and that they are subject to the democratic decision-making process and parliamentary control. Perhaps more importantly, there is also sufficient room for interventions by national courts. Drawing inspiration from the German case, national judges could assign more weight to the vulnerability of welfare beneficiaries as a factor when scrutinising state control measures.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Bellamy, C. et al. (2005) 'Joined-up Government and Privacy in the United Kingdom: Managing Tensions between Data Protection and Social Policy, Part II', *Public Administration (magazine)* 83, 2, 393–415.

Britz, G. (2009) 'Europäisierung des grundrechtlichen Datenschutzes?', *Europäische Grundrechte Zeitschrift (EuGRZ)* 1–12.

Burgkardt, F. (2013) *Grundrechtlicher Datenschutz zwischen Grundgesetz und Europaraecht*, Hamburg: Verlag Dr. Kovă.

Cabinet Office (2016) *National Fraud Initiative Report*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/738282/nfi_national_report_2016.pdf

Cabinet Office (2018) *Code of Data Matching Practice*, published on 18 September.

86. Cf in particular Article 13(2) European Social Charter; the right to social security, including social assistance, is protected Article 9 International Covenant on Economic, Social and Cultural Rights, and Articles 12 and 13 European Social Charter.
87. European Committee of Social Rights (1969), Conclusions I, Statement of interpretation Article 13.

CBP (2006) *Notitie Fraudebestrijding door bestandskoppeling*, Den Haag: College Bescherming Persoonsgegevens https://autoriteitpersoonsgegevens.nl/nl/nieuws/notitie-fraudebestrijding-door-bestandskoppeling

CBP (2007) *Bevindingen ambtshalve onderzoek Waterproof*, Den Haag: College Bescherming Persoonsgegevens https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/uit/z2006-00476.pdf

CBP (2011) *Besluit tot oplegging last onder dwangsom*, Den Haag: College Bescherming Persoonsgegevens https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/pb/pb_20110317-dwangsom-siod.pdf

CBP (2014) *Advies conceptbesluit SyRI*, Den Haag: College Bescherming Persoonsgegevens https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2013-00969.pdf

Daguerre, A and Etherington, D. (2014) *Workfare in 21st Century Britain: The Erosion of Rights to Social Assistance*, London: Middlesex University.

Dwyer, P. (2000) *Welfare rights and responsibilities: Contesting social citizenship*, Bristol: The Policy Press.

Dwyer, P. (2004) 'Creeping Conditionality in the UK: From Welfare Rights to Conditional Entitlements?', *Canadian Journal of Sociology*, 29, 3, 265–287.

Dwyer, P. and Wright, S. (2014) 'Universal Credit, ubiquitous conditionality and its implications for social citizenship', *Journal of Poverty and Social Justice*, 22, 1, pp. 27–35.

Eichenhofer, E. (2015) *The Law of the Activating Welfare State*, Baden-Baden: Nomos.

Fromm, V. (2013) *Kommentar* in: jurisPK-SGB X, § 67 SGB X, Nr. 9; BT-Drs. 8/4022.

Giddens, A. (1998) *The Third Way: The Renewal of Social Democracy*, Cambridge: Polity Press.

Hirschboeck, T. (2004) 'Ausbau automatisierter Datenabgleiche im Bereich der Sozialhilfe', *Zeitschrift für die sozialrechtliche Praxis (ZFSH/SGB)*, 590–595.

Inspectie, SZW. (2012) *Nota van bevindingen Bestandskoppelingen bij fraudebestrijding*, Den Haag: Inspectie Sociale Zekerheid en Werkgelegenheid.

Klingenberg, A. (2016) *Gegevensbescherming in het gemeentelijke sociale domein*, in: Vonk, G (ed.) *Rechtsstatelijke aspecten van de decentralisaties in het sociale domein*, Groningen: Vakgroep Bestuursrecht and Bestuurskunde.

Kunkel, P. (1995) 'Mißbrauchskontrolle oder Kontrollmißbrauch in der Sozialhilfe?', *NVwZ*, 21–24.

Massing, J. (2012) *Ein Abschied von den Grundrechten*, Süddeutsche Zeitung 09.01.2012, 10, available online at https://www.datenschutzbeauftragter-online.de/wp-content/uploads/2012/01/20120109_SZ_Masing_Datenschutz.pdf

Ministerie van Sociale Zaken en Werkgelegenheid (2014) *Verzoek om reactie op berichtgeving over het koppelen van data in verband met fraudeonderzoeken*.

Merten, D. (2018) *Kommentar* in: Giesen, R., Kreikebohm, R, Rolfs, C and Udsching, P, BeckOK Sozialrecht, Ed. 51, Munich: C.H. Beck.

Raad van State. (2014) Advies W12.14.0102/III.

Rodger, JJ. (2008) *Criminalising Social Policy: Anti-social Behaviour and Welfare in a De-civilised Society*, Cullompton: Willan Publishing.

Schmidt, B. (2018) in: *Gagel Kommentar SGB II / SGB III*, Ed. 70, Munich: C.H. Beck.

Schwitters, R. and Vonk, G. (2016) 'Paraticipation Societies or Repressive Welfare States?', in: Comtois, S. and de Graaf, K (eds.) *On Lawmaking and Public Trust,* NILG - *Governance and Recht*, 14, 121–134, Den Haag: Eleven International Publishing.

Silver, H. (2007) *The Process of Social Exclusion: The Dynamics of an Evolving Concept*, Chronic Poverty Research Centre, Working Paper 95.

Vonk, GJ. (2014) 'Repressive Welfare States: The Spiral of Obligations and Sanctions in Social Security', *European Journal for Social Security*, 16, 3, 188–203.

Wachter, S, Mittelstadt, B and Floridi. (2017) 'Why a Right to Explanation of Automated Decision-Making Does not Exist in the General Data Protection Regulation', *Journal of International Data Privacy Law*, 7, 2, 76–99.

Watts, B and Fitzpatrick, S. (2018) *Welfare Conditionality*, London: Routledge.

Westin (1970) *Privacy and freedom*, London: The Bodley Head.

WP29 (2013) Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203.